AGENDA 2019

MES	FECHAS	CURSO	CIUDAD	PUNTOS IMPORTANTES	DIRIGIDO A	HORARIO	INVERSION (*) SIN IVA
MARZO	21 al 23	**LABORATORIO PRACTICO** **ETHICAL HACKING** (24 horas)	UIO	Métodos y técnicas de Hacking, **Principales Ataques y contramedidas.** Revisión de las principales herramientas para identificar y verificar la **vulnerabilidad la seguridad de redes informáticas.** - Entorno Hacking - Buscadores - Ataques hacia el cliente y el servidor - Ataques MiTM - Ataques de ingeniería social - Backdoring	Gerentes Tecnología, Oficial de Seguridad de Informática. Administradores de Seguridad TI. Auditores Informáticos,	09:00 a 18:00 (Jueves a Sábado)	$ 500
ABRIL	12 Y 13	**TALLER ISO 27035** **Gestión de Incidentes de Seguridad de Informacion** (12 horas)	UIO	Comprender el proceso de Gestión de Incidentes de Seguridad de la Información de acuerdo con la directriz internacional ISO 27035. Introducción a Seguridad de Información **Planificación y preparación** • Política y Esquema de gestión de incidentes de seguridad de la información. **Detección y reporte** • Detección y reporte de eventos de seguridad de la información. **Evaluación y decisión** • Revisión de las actividades claves	Gerentes y Oficiales de Seguridad de Información Gerentes de Tecnología (Adm. Servidores, BD, HW, Sw; Redes, Mesa de Ayuda o Help Desk) Auditores IT	09:00 a 18:00 (Viernes) 09:00 a 13h00 (Sábado)	$ 300
MAYO	**INFOSECURITY 2019 - Tour "I'LL BE WATCHING YOU"** Quito 08 Mayo - Hotel Marriott Guayaquil 09 Mayo- Hotel Sherton						
	16 al 18	**LABORATORIO PRACTICO** **Peritaje Informatico y Delitos Informaticos** (20 horas)	GYE	**Reconocimiento legal de la documentación electrónica** que genera las transacciones comerciales (acuerdos, contratos celebrados electrónicamente), de manera que sea posible utilizar esta documentación como medio **probatorio, perfectamente válido en cualquier procedimiento legal y judicial.** -Extracción y análisis de Metadatos bajo línea de comandos - Falsificación de imágenes: comprobación técnica y legal de metadatos. - Peritaje Informático: Forensia vs Informática Forense. - Fases del Peritaje Informático Judicial. - Línea de tiempo. - Extracción de Imagen Forense bajo línea de comandos	Unidad de Riesgos, Directores, Gerentes y Responsables de áreas administrativas, Departamento legal, Departamento seguridad informática, RRHH, Consultores de Tecnología. Auditores IT	09:00 a 18:00 (Jueves y Viernes) 09:00 a 13:00 (Sábado)	$ 500
	23 al 25	**TALLER ISO 27002** **Guias de Implementacion de Control de Seguridad** (20 horas)	UIO	**Domine los principios y conceptos fundamentales de los controles de seguridad de la información basados en las mejores prácticas de la ISO 27002.**	Gerentes y Oficiales de Seguridad de Información, Auditoria IT, Analistas de Riesgos en tecnologías de información, Analistas & Gerentes Continuidad de Negocio.	09:00 a 18:00 (Jueves y Viernes) 09:00 a 13:00 (Sábado)	$ 400

AGENDA 2019

MES	FECHAS	CURSO	CIUDAD	PUNTOS IMPORTANTES	DIRIGIDO A	HORARIO	INVERSION (*) SIN IVA
JUNIO	6 al 9	**TALLER BPM** **Business Process Management** (28 horas)	UIO	La administración de procesos de negocios (BPM) es una disciplina para la administración de las operaciones que utiliza diversos métodos para establecer, modelar, analizar, medir, mejorar, optimizar y automatizar los procesos de negocio.	Gerencias y Jefaturas de Procesos, Gerentes y Jefaturas de Sistemas de Información, Ingenieros y Analistas de Desarrollo, Administradores de Sistemas de Gestión. Analistas de Procesos.	09:00 a 18:00 (Jueves y Sábado) 09:00 a 13:00 (Domingo)	$ 575
JUNIO	21 y 22	**TALLER ISO 22301** **Implementador BCP Continuidad de Negocio** (16 horas)	UIO	Revisar las directrices de ISO 22301 para diseñar Planes de Continuidad de Negocio que **permitan a la organización seguir operando** luego de un **evento inesperado** (Desastres Naturales, Fallas IT, etc). 1. Planificación de GCN (Gestión de Continuidad de Negocio) Definición del Alcance de un BCP Definición de Roles y Responsabilidades 2. Operación de GCN Análisis de Impacto (BIA) Análisis de Riesgos Definición de Estrategias de Recuperación 3. Monitoreo & Medición GCN	Gerencia General, Gerencias de Negocio (Finanzas, RRHH, Procesos, Legal) Gerentes y Oficiales de Seguridad de Información. Gerencia y oficiales de Riesgo	09:00 a 18:00 (Viernes y Sábado)	$ 350
JULIO	18 al 20	**LABORATORIO PRACTICO** **ETHICAL HACKING** (24 horas)	GYE	Métodos y técnicas de Hacking, **Principales Ataques y contramedidas.** Revisión de las principales herramientas para identificar y verificar la **vulnerabilidad la seguridad de redes informáticas.** - Entorno Hacking - Buscadores - Ataques hacia el cliente y el servidor - Ataques MiTM - Ataques de ingeniería social - Backdoring	Gerentes Tecnología, Oficial de Seguridad de Informática. Administradores de Seguridad TI. Auditores Informáticos,	09:00 a 18:00 (Jueves a Sábado)	$ 600
AGOSTO	23 Y 24	**TALLER ISO 27003** **Guías de Implementación SGSI 27001** (16 horas)	GYE	Revisar las directrices de ISO 27003 para el diseño e implementación de un Sistema de Gestión de Seguridad de Información SGSI 27001:2013 • Obtención de la aprobación de la alta dirección para iniciar un SGSI. • Definición del alcance del SGSI, límites y políticas. • Evaluación de requerimientos de seguridad de la información. • Evaluación de Riesgos y Plan de tratamiento de riesgos. • Diseño del SGSI.	Gerencia General, Gerencias de Negocio Gerente y Oficial Seguridad Información Gerentes de Tecnología Auditores IT	09:00 a 18:00 (Viernes y Sabado)	$ 475

AGENDA 2019

MES	FECHAS	CURSO	CIUDAD	PUNTOS IMPORTANTES	DIRIGIDO A	HORARIO	INVERSION (*) SIN IVA
SEPTIEMBRE	20 Y 21	**TALLER ISO 27035** **Gestión de Incidentes de Seguridad de Informacion** (12 horas)	UIO	Comprender el proceso de Gestión de Incidentes de Seguridad de la Información de acuerdo con la directriz internacional ISO 27035. Introducción a Seguridad de Información **Planificación y preparación** • Política y Esquema de gestión de incidentes de seguridad de la información. **Detección y reporte** • Detección y reporte de eventos de seguridad de la información. **Evaluación y decisión** • Revisión de las actividades claves **Respuestas** • Respuesta inmmediata, posteriores, escalamiento, registro.	Gerentes y Oficiales de Seguridad de Información Gerentes de Tecnología (Adm. Servidores, BD, HW, Sw; Redes, Mesa de Ayuda o Help Desk) Auditores IT	09:00 a 18:00 (Viernes) 09:00 a 13h00 (Sábado)	$ 300
OCTUBRE	24 al 26	**LABORATORIO PRACTICO** **Peritaje Informatico y Delitos Informaticos** (20 horas)	UIO	**Reconocimiento legal de la documentación electrónica** que genera las transacciones comerciales (acuerdos, contratos celebrados electrónicamente), de manera que sea posible utilizar esta documentación como medio **probatorio, perfectamente válido en cualquier procedimiento legal y judicial.** -Extracción y análisis de Metadatos bajo línea de comandos - Falsificación de imágenes: comprobación técnica y legal de metadatos. - Peritaje Informático: Forensia vs Informática Forense. - Fases del Peritaje Informático Judicial. - Línea de tiempo. - Extracción de Imagen Forense bajo línea de comandos	Unidad de Riesgos, Directores, Gerentes y Responsables de áreas administrativas, Departamento legal, Departamento seguridad informática, RRHH, Consultores de Tecnología. Auditores IT	09:00 a 18:00 (Jueves y Viernes) 09:00 a 13:00 (Sábado)	$ 450
NOVIEMBRE	22 y 23	**TALLER ISO 27003** **Guías de Implementación SGSI 27001** (16 horas)	UIO	Revisar las directrices de ISO 27003 para el diseño e implementación de un Sistema de Gestión de Seguridad de Información SGSI 27001:2013 • Obtención de la aprobación de la alta dirección para iniciar un SGSI. • Definición del alcance del SGSI, límites y políticas. • Evaluación de requerimientos de seguridad de la información. • Evaluación de Riesgos y Plan de tratamiento de riesgos. • Diseño del SGSI.	Gerencia General, Gerencias de Negocio Gerente y Oficial Seguridad Información Gerentes de Tecnología Auditores IT	09:00 a 18:00 (Viernes y Sábado)	$ 350
DICIEMBRE	9 y 10	**TALLER ISO 27005** **Gestión de Riesgo en Seguridad de Información** (16 horas)	UIO	Revisar las directrices de ISO 27005 para identificar y clasificar activos de información, identificar amenazas y vulnerabilidades y calcular riesgos en el ámbito de la seguridad de información. • Cómo identificar y categorizar los activos de información. • Cómo valoramos los activos en base a la Confidencialidad, Integridad y Disponibilidad.	Gerencia General, Gerencias de Negocio Gerentes y Oficiales de Seguridad de Información. Gerencia y oficiales de Riesgo Gerentes de Tecnología	09:00 a 18:00 (Viernes y Sábado)	$ 350

La programación de cursos está sujeta al cupo mínimo de estudiantes requerido para cada curso.

Estos cursos pueden ser dictados In-Company según las necesidades de su empresa.